UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/768,425	01/30/2004	Dan Flowers	100.644US01	6962

34206 7590 11/05/2007

FOGG & POWERS LLC
10 SOUTH FIFTH STREET
SUITE 1000
MINNEAPOLIS, MN 55402

EXAMINER	
MIA, HASSEN A	
ART UNIT	**PAPER NUMBER**
4131	

NOTIFICATION DATE	DELIVERY MODE
11/05/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@fogglaw.com

Office Action Summary	Application No.	Applicant(s)	
	10/768,425	FLOWERS ET AL.	
	Examiner	Art Unit	
	Hassen A. Mia	2609	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 28 rejected under 35 U.S.C. 101 because, the claimed invention is directed to non-statutory subject matter. Claim 28 is directed towards data structure, which is not patentable.

Claim rejections – 35 USC § 102

The following is a quotation of the appropriate paragraphs of U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person should be entitled to a patent unless-

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim 1 - 16 are rejected under 35 U.S.C. 102(e) as being anticipated by Kung et al. US Patent: 6,563,797, (hereafter refer Kung).

Regarding claim1, Kung teaches IP voice call surveillance through use of non-dedicated IP phone with signal alert provided to indicate content of incoming call prior to an answer as being A.

- "receiving a data packet intended for transmission to a first recipient" (col. 2, lines 56 – 65), the initiation of a call to an IP telephone having a known DN (destination number) step 203, where IP calls inherently user packets).
- "storing the data packet in a buffer", (watchdog program), (fig. 2, item 207, where step 207 inherently requires storage while processing, i.e., for inquiry and copying).
- "transmitting the data packet to the first recipient" (col. 2, lines 59 – 65, a for monitored and non-monitored calls packets are sent on to the original destination).
- "determining whether the data packet is flagged for surveillance and, if so, transmitting the data packet to a second recipient", (col. 2, lines 60 through col. 3, line 14, decision block 207 an inquiry asks if the call DN is one of a list of IP telephone under surveillance).
- "releasing the buffer such that another data packet can be stored therein", (the watchdog program inherently releases the buffer after copying a packet).

Regarding claim 2, Kung teaches, "the method of claim 1, further comprising, before transmitting the data packet to the first recipient, determining whether the data packet should be flagged for surveillance", (fig. 2, step 207, determines if it is on the surveillance list).

Regarding claim 3, the method of claim 2, Kung teaches, "wherein determining whether the data packet should be flagged for surveillance comprises determining whether the data packet is being transmitted to or from a telecommunications device

associated with an electronic surveillance protocol (ESP) object", col. 3, lines 5 – 10, in the instance of the gateway of the monitoring IP telephone the gateway in one embodiment rings the monitoring IP telephone with a distinctive ring, as per block 215, to indicate to the party answering the phone that this is a call connection for the purpose of eavesdropping in on the target IP telephone.

Regarding claim 4, the method of claim 3, Kung teaches, "wherein the telecommunications device comprises an IP phone", fig. 2, step 211, both monitored and monitoring IP telephones.

Regarding claim 5, the method of claim 1, Kung teaches, "wherein the data packet is received over a hybrid fiber-coax (HFC) network", fig. 1 element 105, HFC distribution plant.

Regarding claim 6, the method of claim 1, Kung teaches, "wherein the data packet is received over a public switched telephone network (PSTN)", fig. 1, the public switch telephone network element 115.

Regarding claim 7, the method of claim 1, Kung teaches, "wherein the data packet comprises a surveillance flag segment, a header segment, and a data segment", fig. 2, step 211, IP-AMCP locates IP addresses of both monitored and monitoring IP telephones.

Regarding claim 8, the method of claim 1, Kung teaches, "wherein the data packet is transmitted to the first recipient over a HFC network", fig. 1, HFC distribution plant element 105.

Regarding claim 9, the method of claim 1, Kung teaches, "wherein the data packet is transmitted to the first recipient over a PSTN", fig. 1 element 115.

Regarding claim10, the method of claim 1, Kung teaches, "wherein determining whether the data packet is flagged for surveillance comprises referencing a surveillance flag segment of the data packet", fig. 2, step 211, IP-AMCP locates IP addresses of both monitored and monitoring IP telephones.

Regarding claim 11, the method of claim 1, Kung teaches, "wherein transmitting the data packet to the second recipient comprises transmitting the data packet to a delivery function module (DF)", fig. 2, step 213, IP-AMCP sends a distinctive alert message to IP gateway servicing monitoring IP telephone.

Regarding claim 12, Kung teaches:

- Kung teaches, "storing a data packet in a buffer, wherein the data packet comprises a header segment having a first destination address; (watchdog program), (fig. 2, item 207, where step 207 inherently requires storage while processing, i.e., for inquiry and copying).
- "transmitting the data packet to a recipient at the first destination address", col. 2, lines 62 – 65, if it is not the flow proceeds per the instructions of block 209 to handle the call as a non-monitored call and the process ends at terminal 219.
- "replacing the first destination address in the header segment of the data packet with a second destination address", col. 2, lines 66 – 67 through col. 3 line 1, if the DN called is on the surveillance list the process as per block 211 locates the addresses of the calling and called Dens in the IP-AMCP.

- "transmitting the data packet to a recipient at the second destination address", col. 3, lines 1 – 5, According to the instructions of block 213 the IP-AMCP sends a distinctive alert message to a gateway terminal connecting the target IP telephone to the IP network and also to the gateway serving the monitoring IP telephone.
- "after transmitting the data packet to the recipient at the second destination address, releasing the buffer such that another data packet can be stored therein", (the watchdog program inherently releases the buffer after copying a packet).

Regarding claim 13, the method of claim 12, Kung teaches, "wherein the recipient at the first destination address is the intended recipient of the data packet, and the recipient at the second destination address is a law enforcement official"' col. 1, lines 11 – 14, this invention relates to surveillance of telephone calls over a public communications link and is particularly concerned with providing assistance for such surveillance to law enforcement agencies.

Regarding claim 14, the method of claim 12, Kung teaches, "wherein transmitting the data packet to the recipient at the first destination address comprises transmitting the data packet over a HFC network", fig. 1, HFC distribution plant element 105.

Regarding claim 15, the method of claim 12, Kung teaches, "wherein transmitting the data packet to the recipient at the first destination address comprises transmitting the data packet over a PSTN", fig. 1, the public switch telephone network element 115.

Regarding claim 16, the method of claim 12, Kung teaches, "wherein the data packet further comprises a surveillance flag segment and a data segment", fig. 2, step 211, IP-AMCP locates IP addresses of both monitored and monitoring IP telephones.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims, 17 - 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Kung in view of Thomas H. Cormen Introduction to Algorithms (hereafter refer Cormen).

Regarding claim 17, Kung teaches,

- "receiving an instruction to create a new (.....) stored in a memory of a cable modem termination system (CMTS)(CMB)", col. 1, lines 57 – 60, a cable modem bank (CMB) or an IP Phone intercept List (IP-PIL) lists the IP phones to be monitored and responds when one of those listed phones to be monitored becomes active.
- "generating (.....) entry comprising information about an end-to-end connection between a subscriber using an IP phone and another party", col. 3, lines 1 – 5, According to the instructions of block 213 the IP-AMCP sends a distinctive alert message to a gateway terminal connecting the target IP telephone to the IP network and also to the gateway serving the monitoring IP telephone.
- "determining whether transmissions to or from the IP phone are subject to surveillance and, if so, adding surveillance information to the ..... col. 2, lines 66

– 67 through col. 3, line 1, If the DN called is on the surveillance list the process as per block 211 locates the addresses of the calling and called Dens in the IP-AMCP.

- Kung does not teach "receiving an instruction to **create** (insert) **a new hash entry in hash entry table** stored in a memory of a cable modem termination system (CMTS)", however, Cormen teaches, that many applications require a dynamic set (hash table) that supports only the dictionary (database) operations Insert, (Introduction to Algorithm page 221).
- Kung does not teach "generating (search) **a hash entry** comprising information about an end-to-end connection between a subscriber using an IP phone and another party", however, Cormen teaches, that many applications require a dynamic set (hash table) that supports only the dictionary (database) operations Insert, (Introduction to Algorithm page 221).
- "determining whether transmissions to or from the IP phone are subject to surveillance and, if so, adding surveillance information to the **hash entry**.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Kung's IP voice call surveillance by using hash table since hash table is an effective data structure for implementation a dictionaries/databases.

Regarding claim 18, the method of claim 17, Kung teaches, "wherein the instruction to create a new hash entry is received when a telephone call is initiated with a subscriber using an IP phone", col. 2, lines 59 – 61, a WatchDog program associated with the IP-AMCP notes that the call is being initiated as per block 205.

Regarding claim 19, the method of claim 17, Kung teaches, "wherein determining whether transmissions to or from the IP phone are subject to surveillance comprises determining whether an ESP object is associated with the IP phone", col. 3, lines 5 – 10, in the instance of the gateway of the monitoring IP telephone the gateway in one embodiment rings the monitoring IP telephone with a distinctive ring, as per block 215, to indicate to the party answering the phone that this is a call connection for the purpose of eavesdropping in on the target IP telephone.

Regarding claim 20, the method of claim 17,Kung teaches, "wherein the surveillance information comprises the destination address of a DF", col. 2, lines 66 – 67 through col. 3, line 1, If the DN called is on the surveillance list the process as per block 211 locates the addresses of the calling and called DNs in the IP-AMCP.

Claims, 21 – 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Kung in view of Dikmen et al. US Publication No.: 2003/0078041 (hereafter refer Dikmen).

Regarding claim 21, Kung teaches CM (cable modem) comprising:

- Kung teaches, "a buffer configured to store data packets", (watchdog program), (fig. 2, item 207, where step 207 inherently requires storage while processing, i.e., for inquiry and copying).
- Kung teaches, "a memory configured to store (.....) entry table, wherein the (....) entry table includes information regarding whether data packets should be marked for surveillance" (col. 2, lines 60 through col. 3, line 14, decision block

207 an inquiry asks if the call DN is one of a list [necessarily stored in memory] of IP telephone under surveillance).

However, Kung does not specifically teach "a memory configured to store a **hash** entry table, wherein the **hash** entry table includes information (....)", however, Cormen teaches, the use of a hash table to access dictionary entries including the ability to insert [store] a new entry, (Introduction to Algorithm page 221, paragraph 1).

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Kung's IP voice call surveillance by using hash table since hash table is an efficient data structure for implementation a dictionaries/databases, (Introduction to Algorithm page 221, paragraph 1, lines 5 - 6).

- Kung teaches "a processor coupled to the buffer and to the memory configured to transmit data packets to their intended recipients, wherein the processor comprises a surveillance module configured to determine whether a given data packet is marked for surveillance and, if so, transmit the data packet to a surveilling recipient, col. 2, lines 59 – 62 and lines 66 – 67, col. 3 lines 1 – 5.

But, Kung does not specifically teach "a processor coupled to, wherein the processor comprises a surveillance module configured to determine whether a given data packet is marked for surveillance and, if so, transmit the data packet to a surveilling recipient **without** creating a copy of the data packet. However, Dikmen teaches, redirecting a call without copying such as forward or divert or deflect, paragraph 0019.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Kung's IP voice call surveillance by using redirecting of calls technique as taught

by Dikmen for the purpose of dealing with the suspicious caller directly by acting as the intended recipient.

Regarding claim 22, the CMTS (CMB) of claim 21, Kung teaches, "further comprising a cable port in communication with the processor through a cable receiver and a cable transmitter, wherein the cable port is configured to receive transmissions over a HFC network", fig. 1, HFC distribution plant element 105.

Regarding claim 23, the CMTS (CMB) of claim 21, Kung teaches, "further comprising a network port in communication with the processor through a network receiver and a network transmitter, wherein the network port is configured to receive transmissions over a PSTN", fig. 1, the public switch telephone network element 115.

Regarding claim 24, the CMTS (CMB) of claim 21, Kung teaches, "wherein each data packet comprises a surveillance flag segment, a header segment, and a data segment", fig. 2, step 211, IP-AMCP locates IP addresses of both monitored and monitoring IP telephones, all IP packets have header and data segments.

Regarding claim 25, the CMTS (CMB) of claim 21, Kung teaches, "wherein the surveillance module is configured to determine whether data packets transmitted to or from an IP phone should be marked for surveillance", col. 1, lines 57 – 60, in an IP telephone environment, a cable modem bank (CMB) or an IP Phone intercept List (IP-PIL) lists the IP phones to be monitored and responds when one of those listed phones to be monitored becomes active.

Regarding claim 26, the CMTS (CMB) of claim 25, Kung teaches, "wherein the surveillance module determines whether data packets should be marked for

surveillance by determining whether an ESP object is associated with the IP phone", col. 1, lines 21 – 25, reciting requirements for assuring law enforcement access to electronic communications. Such access is required to be in real time, have full time monitoring capabilities, simultaneous intercepts, and feature service descriptions.

Regarding claim 27, the CMTS of claim 21, Kung teaches, "wherein the surveillance module determines whether a data packet is marked for surveillance by referencing surveillance flag segment of the data packet", col. 2, lines 61 – 61, in decision block 207 an inquiry asks if the called DN is one of a list of IP telephone under surveillance.

Claims, 29 - 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Kung in view of well known in the art

Regarding claim 29, a machine-readable medium comprising machine-readable instructions for causing a computer to perform a method,

Kung in his IP voice surveillance through us of non-dedicated IP hone with signal alert provided to indicate on incoming call prior to an answer as being a monitored call teaches,

- "receiving a data packet intended for transmission to a first recipient" (col. 2, lines 56 – 65), the initiation of a call to an IP telephone having a known DN (destination number) step 203, where IP calls inherently user packets).
- "storing the data packet in a buffer", (watchdog program), (fig. 2, item 207, where step 207 inherently requires storage while processing, i.e., for inquiry and copying).

- "transmitting the data packet to the first recipient", (col. 2, lines 59 – 65, a for monitored and non-monitored calls packets are sent on to the original destination).
- "determining whether the data packet is flagged for surveillance and, if so, transmitting the data packet to a second recipient", (col. 2, lines 60 through col. 3, line 14, decision block 207 an inquiry asks if the call DN is one of a list of IP telephone under surveillance).
- "releasing the buffer such that another data packet can be stored therein", (the watchdog program inherently releases the buffer after copying a packet).

Kung does not specifically teach the use of machine or CPU. Examiner takes Official Notice that implementing software to do the process is well known in the art.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Kung's IP voice call surveillance system by implementing a software processing for the purpose of the flexibility of programs and reducing cost.

Regarding claim 30, the machine-readable medium of claim 29, Kung teaches, "wherein the method further comprises, before transmitting the data packet to the first recipient, determining whether the data packet should be flagged for surveillance", fig. 2, step 207, determines if it is on the surveillance list.

Regarding claim 31, the machine readable medium of claim 30, Kung teaches, "wherein determining whether the data packet should be flagged for surveillance comprises determining whether the data packet is being transmitted to or from a telecommunications device associated with an ESP object", col. 3, lines 5 – 10, in the

instance of the gateway of the monitoring IP telephone the gateway in one embodiment rings the monitoring IP telephone with a distinctive ring, as per block 215, to indicate to the party answering the phone that this is a call connection for the purpose of eavesdropping in on the target IP telephone.

Regarding claim 32, the machine readable medium of claim 31, Kung teaches, "wherein the telecommunications device comprises an IP phone", fig. 2, step 211, both monitored and monitoring IP telephones.

Regarding claim 33, the machine-readable medium of claim 29, Kung teaches, "wherein the data packet is received over a HFC network", fig. 1 item 105, HFC distribution plant.

Regarding claim 34, the machine readable-medium of claim 29, Kung teaches, "wherein the data packet is received over a PSTN", fig. 1, the public switch telephone network element 115.

Regarding claim 35, the machine readable medium of claim 29,Kung teaches, "wherein the data packet comprises a surveillance flag segment, a header segment, and a data segment", fig. 2, step 211, IP-AMCP locates IP addresses of both monitored and monitoring IP telephones.

Regarding claim 36, the machine readable medium of claim 29, Kung teaches, "wherein the data packet is transmitted to the first recipient over a HFC network", fig. 1, HFC distribution plant element 105.

Regarding claim 37, the machine readable medium of claim 29, Kung teaches, "wherein the data packet is transmitted to the first recipient over a PSTN", fig. 1, the public switch telephone network element 115.

Regarding claim 38, the machine readable medium of claim 29, Kung teaches, "wherein determining whether the data packet is flagged for surveillance comprises referencing a surveillance flag segment of the data packet", fig. 2, step 211, IP-AMCP locates IP addresses of both monitored and monitoring IP telephones.

Regarding claim 39, the machine-readable medium of claim 29, Kung teaches, "wherein transmitting the data packet to the second recipient comprises transmitting the data packet to a DF", fig. 2, step 211, IP-AMCP locates IP addresses of both monitored and monitoring IP telephones.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- **Suprunov US Patent No. 6,405,030** teaches, (system for interception of digital cellular phone communication).
- **Maillet et al. US Patent No. 6,424,701** teaches, (Method and equipment of interception).
- **Magnusson US Patent No. 6,122,499** teaches, (system and/or method for call intercept capability in a global mobile satellite communications system).
- **Dikmen US Pub. No.: 2003/00108182** teaches, (Method and apparatus for intercept o wire line communication).

- **Mukherjee et al. US Patent No. 6,449,474** teaches, (method and apparatus for call interception capability for use with intelligent network services).
- **Pyke et al. US Pub. No.: 2003/0179747** teaches, (System and method for intercepting telecommunications).
- **Blanchard et al. US Patent No. 6,141,548** teaches, (method and apparatus for location based intercept in a communication system).
- **Sjoblom US Publication No. 2002/0150096** teaches, (ordered delivery of intercepted data).
- **Bondy et al. US Patent No.: 7,006,508** teach, (communication network with a collection gateway and method for providing surveillance service).
- **Porras et al. US Patent No.: 6,321,338** teach, (network surveillance).
- **Haumont US Patent No.: 6,654,589** teach, (legal interception in a telecommunication network).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hassen A. Mia whose telephone number is 571-272-9749. The examiner can normally be reached on M-F 7:30AM - 5:00PM EST alt. Friday off. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Brian Pendleton can be reached on 571-272-7527. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HM

BRIAN TYRONE PENDLETON
SUPERVISORY PATENT EXAMINER